Control system cyber security-maintaining the reliability of the critical infrastructure

Testimony of Joseph M. Weiss, control system cyber security expert before the Committee on Government Reform's Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, U.S. House of Representatives on July 24, 2002.

Washington, D.C. -- Thank you for the opportunity to address this committee on what I consider to be a very important topic-the cyber security of the critical industry infrastructures.

Since September 11th, the focus of security in the United States has been on physical terrorist attacks. Cyber security concerns have been directed toward Internet use and networking technology. Dramatic steps are being taken to ensure security against physical attacks and increased emphasis is being placed on securing the Internet and networking systems for traditional IT business systems. However, the same cannot be said for operational control systems. These are the distributed control systems (DCS), programmable logic controllers (PLC), and supervisory control and data acquisition (SCADA) systems that are utilized as the backbone of the global industrial infrastructure. There are only a limited number of suppliers of these systems and they are sold throughout the world. Applications include electric power, water, oil and gas, chemicals, pharmaceuticals, paper, metals refining, auto manufacturing, and food processing. There is a growing threat that cyber attacks on operational control systems could create a crisis for which no one is prepared.

The Threat

Whether security breaches come from organized terrorist attacks, hackers, or even unintentional break-ins, the potential exists for devastating consequences. Yet cyber security in control systems is inadequately being addressed by regulatory agencies and the industries themselves.

Cyber attacks on control systems can be targeted at specific systems or subsystems and can target multiple locations simultaneously from a remote location. Such attacks can directly challenge equipment design and safety limits, causing system malfunctions and shutdowns. Electronic attacks can even impact restoration efforts by manipulating procedures or dynamically changing equipment conditions.

Various cyber security intrusion studies by the Department of Energy and commercial security consultants have demonstrated the cyber vulnerabilities of these systems to unauthorized access. Moreover, many control systems have been designed with architectures that did not account for the wholesale transition from analog to digital instrumentation or external interfaces to corporate and other outside entities. Consequently, these systems lack the bandwidth to operate reliably in today's environments. There have been several cases where control systems (SCADA and DCS) have had denial of service events because of their lack of control system robustness. Procedures on how to utilize these systems in an appropriate manner are often lacking.

As a result, there have been several cases of denial of service on control systems, including in a nuclear facility, because of inadequate procedures.

Background

Networking technology (Ethernet, LANs, and WANs) and the use of the Internet are ubiquitous. This technology (open, standards-based networking) was initially applied to business systems and other communication systems where timing was not critical, and the "store and forward" approach was routine or expected. Because it was also recognized that these systems would be sending confidential information over unsecured networks, electronic security was part of the system or application design early in the development of the technology. Process and plant operational systems such as "real time" plant control and SCADA systems were originally designed as proprietary, stand-alone systems where security was provided by physical isolation and limited access control (that is, log-on identification). Now, deregulation, productivity enhancements, corporate desire for control system information through such tools as Enterprise Resource Planning (ERP), and other changes are mandating enormous increases in information sharing. The electric power and other traditionally "isolated" industries are adopting more open, standards-based networking technology and/or the Internet to provide increased information sharing in their operations. It has been assumed that the information will be secure and all users would be trusted users.

Electronic vulnerabilities in operational systems are created by a variety of factors including:

Equipment suppliers provide modems for remote access as part of their standard system configuration and utilize default passwords.
Plant staffs are reluctant to change default passwords because of operator performance considerations during emergency events.
Plant and corporate staff use of remote access tools such as PCAnywhere or XWindows.
Security patches often are not supplied to the end-users or are not applied for fear of impacting system performance.
Most new control and diagnostic hardware and software are web-enabled.
Control system networks utilize Internet-based control and diagnostic applications without IT Security being aware.
Power marketers use the Internet to access DCS and SCADA systems for real-time information.
Insecure communication protocols exist between control systems.
Applications of tools such as ActiveX controls are insecure.</ul>

Control Systems are Different than IT Systems

The prevailing belief has been that information security technologies, policies, procedures, and standards developed for traditional IT business systems would apply to all systems using networking technologies. However, it has been demonstrated that the real-time nature of operational control systems creates a different set of conditions that has not been adequately addressed by more traditional IT technology approaches.

Traditional IT business systems are non-deterministic and communicate peer-to-peer. Consequently, tasks are performed in a linear manner. This allows these systems to utilize existing security technology such as block encryption algorithms.

Control systems, on the other hand, are deterministic systems, and can communicate in multiple ways such as peer-to-peer, one-to-many, many-to-many, etc. A deterministic system is one where processing tasks occur within specific time intervals and processing tasks receive priorities given by the Real-time Operating System (RTOS). These priorities can change during the process. More importantly, timing within each task is constrained and tasks must be performed and completed before the results are needed-faster than the "real-time" process they are controlling.

Several issues that impact information security technology are inherent in control systems.
Timing:

> Timing is sensitive, not only for the entire process, but also within each task.
> Tasks, and processes within each task, must be capable of being interrupted and restarted.
> Time delays are unacceptable.
> Reliability of data, data packets, etc. is crucial.
> Minimal resources are available.
> Timing and task interrupts can preclude the use of conventional encryption block algorithms.

Communications:

> Non peer-to-peer communications can preclude the use of digital certificates (timing and resources are also issues that could preclude use of digital certificates for control system applications).

Data Integrity:

> Data integrity is crucial; confidentiality is secondary.

Applying IT security technology in control systems can actually impact performance. Several control system suppliers tried to implement National Institute of Standards & Technology (NIST)-approved encryption algorithms on their systems in a test environment. The algorithms were not designed for the timing issues in control system applications. Consequently, the encryption algorithms impacted the control system timing functions to the point the control systems could not perform their functions.

Control System Vulnerabilities
Many forms of remote access have created control system vulnerabilities to security breaches. Insecure communication protocols between control systems and insecure

applications of tools, such as ActiveX controls, cause further risks. Damage can range from loss of confidential data to altering data resulting in erroneous equipment operation or operator information leading to miss-operation. Since operational systems are unique compared to traditional information systems, threats will most likely be from individuals who already understand control systems.

An oft-stated remark is that "when my neighbor gets hit, I will do something." This raises two important points:

> Many facilities have no firewalls or intrusion detection systems. Consequently, they have no means of detecting an electronic intrusion. If they are "hit," the only indication will be the damage caused by the intrusion (this means that the statistics that have been quoted about intrusions do not apply to control systems).
>
> Control systems have been hacked and, in several instances, damage has occurred. Unlike traditional IT electronic attacks that can be identified and categorized by different computer security organizations, there currently is no process to identify and collect potential control system electronic intrusions.

Control systems generally utilize two operating systems. One is at the operator station that has the capability for role-based access, encryption, and other information security technologies. The other is at the "distributed processing unit," where the sensor information is collected and calculations made in real-time. These RTOS are usually proprietary systems that have been configured with specific prioritization and communication threads. Information security policies have not been included in the kernel of these systems. Consequently, these RTOS do not have the capability to make the requisite calls to authorize, authenticate, or encrypt/decrypt before data is sent. Additionally, RTOS dedicate most of their resources to performing calculations related to system operational performance. Security is viewed as an overhead function.

Control System Issues with Existing Security Technology

Security for control systems faces several specific technological hurdles before the energy and other industries will be protected.

Operating Systems

Security standards and policies need to be incorporated into real-time operating systems. However, incorporating security into the control systems means addressing the timing and task completion/interrupt requirements inherent in control system operations. Currently, there are no requirements for computing resources necessary to implement security technology. The Open Group's Real-time Security Forum (with U.S. Department of Defense participation) is addressing this issue.

Encryption

Current block encryption technology "scrambles" the information of an IT system, but it does not let the user know if the information is correct. Standard encryption works in blocks, which do not address the operational system's timing and interrupt needs. Also, existing encryption solutions do not authenticate the source of the data, an important component for ensuring data integrity when packets of data go from one system to the next.

Stream Ciphers, an encryption solution that lets the system encrypt the information as it is received instead of in one batch, has been developed, but still needs to be refined and demonstrated in process controls applications.

Firewalls

Firewalls ensure that the data is coming from a credible source and accepted address, but do not account for data corruption that could occur prior to leaving the control system environment and entering the network. Control systems are custom designed to work between different systems and control the process based on past or expected process experience. Firewall solutions for operating systems would have to determine if the packet information has been corrupted to ensure data integrity.

Intrusion Detection Systems (IDS)

Current IDS solutions were designed to look for the patterns of a traditional Internet-based IT security breach. IDS solutions have not been designed to meet the needs of control systems, which would have to differentiate between an attack and a process change or problem. Digital fault recorders, transient recorders, scan logs, and alarm recorders monitor abnormalities within the process but not the information system logs. Extending existing state models may provide a starting point that can be used with advanced processing technology such as agents.

Protocols

Protocols in use now were designed to make system interactions as easy and open as possible, which leaves traditional security measures such as authentication and authorization out of the loop. Operating systems will have to find protocols that encourage security while still allowing open communication. A number of groups are exploring working solutions, including: International Electrotechnical Commission Technical Committee 57, Working Group 15; the DNP Working Group; and NIST's Process Controls Security Requirements Forum.

What Needs to be Done

Awareness

Awareness of cyber security control system vulnerability is very low. Cyber security has been viewed as an IT and Internet concerns. The IT community does not understand the technical differences between IT and controls. To date, the IT community has not felt the controls market was sufficiently large to engage it. The controls community understands controls. The IT security community understands IT security. There needs to be a "marriage," and it will probably require government "help." This same thought is extended to the funding being made available on cyber security. It is not addressing control systems. Either funding needs to be redirected or new funding needs to be made available to encompass control systems.

There currently have been no overt "drivers" such as regulation or insurance to grab the industry's attention. The Federal Energy Regulatory Commission (FERC) Notice of Public Rulemaking that includes security will hopefully change that view for the utility industry.

Technology Development
There are a number of issues that are under this umbrella.

> Control system security technology R&D. This would entail development of firewalls, intrusion detection, encryption, and other technology specifically for control systems.
> Establishment of control system cyber security test beds. This would be for developing and evaluating new technology, understanding the potential consequences of cyber intrusions, and understanding what technology is really needed. This can only be done in "field conditions" as opposed to a traditional laboratory setting. DOE could be the focal point.
> Establishment of a "CERT" for control systems. Carnegie-Mellon's CERT is not set up to monitor control system intrusions or events. An industry-wide "CERT for control systems" could gather information from the various industries that all use the same technology, making industry-specific Information Sharing and Analysis Centers (ISACs) more useful. This could help dispel the various myths circulating that are not helping the awareness effort. Again, DOE could play an integral part.
> Extension of NIST Common Criteria methodology for industrial control systems. This will enable vendors and end-users to confidently verify that their systems meet security requirements. NIST would be an important participant since this builds on existing NIST methodology.
> Procedure development to secure appropriate interface control. Refinement of generic procedures and development of additional procedures to cover appropriate remote access and interfaces must be completed systematically.
> Control System Cyber Security Standards. Standards need to be developed to address security in an information-sharing environment. NIST would play an important role in this effort.

I am concerned that without taking these actions, our critical infrastructures will be vulnerable to intentional, or even unintentional, events in ways we have not contemplated. Thank you for your time and attention. I would be happy to answer questions.

Joseph M. Weiss, P.E., is an Executive Consultant with KEMA Consulting where he serves as a leading expert on control system cyber security. He can be reached at jweiss@kemaconsulting.com. KEMA Consulting, a subsidiary of KEMA, is an international corporation with more than 450 energy specialists. Assisting over 500 clients in more than 70 countries, KEMA Consulting is a premier provider of total business solutions for the energy industry. More information on KEMA Consulting can be found at www.kemaconsulting.com.